

PCT/JP 03/09894

04.08.03

日 本 国 特 許 庁
JAPAN PATENT OFFICE

REC'D 19 SEP 2003

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2002年 8月 5日

出 願 番 号
Application Number: 特願2002-227888
[ST. 10/C]: [JP 2002-227888]

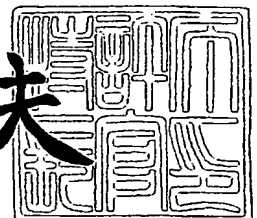
出 願 人
Applicant(s): 財団法人大阪産業振興機構

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 9月 4日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 23526

【提出日】 平成14年 8月 5日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14

【発明の名称】 データ処理方法、データ処理装置、コンピュータプログラム、及び記録媒体

【請求項の数】 7

【発明者】

 【住所又は居所】 大阪府茨木市美穂ヶ丘 5 番 1 号 大阪大学内

 【氏名】 齊藤 和典

【特許出願人】

 【識別番号】 801000061

 【氏名又は名称】 財団法人大阪産業振興機構

【代理人】

 【識別番号】 100078868

 【弁理士】

 【氏名又は名称】 河野 登夫

 【電話番号】 06(6944)4141

【選任した代理人】

 【識別番号】 100114557

 【弁理士】

 【氏名又は名称】 河野 英仁

 【電話番号】 06(6944)4141

【手数料の表示】

 【予納台帳番号】 001889

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0117254

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理方法、データ処理装置、コンピュータプログラム、及び記録媒体

【特許請求の範囲】

【請求項1】 複数の命令コードを含むデータの入力を受付け、受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理方法において、

分岐命令に係る命令コードを前記データから検索し、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶し、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断し、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断することを特徴とするデータ処理方法。

【請求項2】 複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

分岐命令に係る命令コードを前記データから検索する手段と、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶する手段と、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断する手段と、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶する手段と、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する手段と、前記呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にある場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

【請求項3】 前記命令コード群の復帰先アドレスに所定の文字列が対応付

けられているか否かの判断をする手段を更に備え、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力すべくしてあることを特徴とする請求項2に記載のデータ処理装置。

【請求項4】 複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

所定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断する手段と、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

【請求項5】 複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、

所定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コードが検索された場合、前記命令コード群の復帰先アドレスを取得するための命令コードが前記命令コード群に含まれるか否かを判断する手段と、前記命令コードが前記命令コード群に含まれる場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とするデータ処理装置。

【請求項6】 コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムにおいて、

コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判

断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有することを特徴とするコンピュータプログラム。

【請求項 7】 コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体において、

コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有するコンピュータプログラムが記録されていることを特徴とするコンピュータでの読取りが可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、不正な処理を実行するデータを検出するデータ処理方法、データ処理装置、該データ処理装置を実現するためのコンピュータプログラム、及び該コンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体に関する。

【0002】

【従来の技術】

インターネット網の普及に伴い、各種の情報処理装置がコンピュータウィルス、クラッキング等の攻撃の対象となり、それらの脅威に晒される可能性が高くなってきている。

例えば、近年、「ニムダ」、「コードレッド」等のコンピュータウィルスに代表されるように、システムプログラム又はウェブブラウザのようなアプリケーションプログラムの脆弱性（セキュリティホール）を利用して自己増殖させ、甚大な被害を与えたケースが存在する。

【0003】

前述のようなコンピュータウィルス、クラッキング等による攻撃では、不正な処理を行う命令コード（以下、不正コードという）を含む攻撃データを攻撃対象であるサーバ装置、パーソナルコンピュータ等の情報処理装置に対して送信し、その情報処理装置にて前記命令コードが実行されるようにしている。このような攻撃手法は様々なものが存在し、その1つとしてバッファオーバーフローによる攻撃手法が知られている。バッファオーバーフローでは、スタック内に確保されたバッファにおいて、確保されたバッファ以上のスタックエリアに書込みが行われている状態であり、バッファオーバーフローの状態に陥った場合、予期せぬ変数破壊を招き、プログラムの誤動作の原因となり得る。バッファオーバーフローによる攻撃では、プログラムの誤動作を意図的に引き起し、例えばシステムの管理者権限を取得することが行われる。

【0004】

これらのコンピュータウィルス、クラッキング等の攻撃に対処するため、従来では、受信したデータに対して不正コードにみられる特定のビットパターンの有無を検出する。そして、そのようなビットパターンが受信したデータに含まれている場合には、不正コードを含んだ攻撃データであると判定し、データの受信拒否、ユーザへの報知等の処理を行うようにしている。

【0005】

【発明が解決しようとする課題】

そのため、従来の手法により様々なコンピュータウィルス、クラッキング等の攻撃に対処するためには、各コンピュータウィルス、クラッキングに対応した特

定のビットパターンをデータベースに記憶させて予め用意しておく必要があり、新種のコンピュータウイルス、クラッキング手法が発見された場合には、前記データベースを更新して対処しなければならない。

【0006】

ところで、攻撃データに対する従来の検出方法では、前述のように既知のビットパターンを検出するか、又はNOP命令（NOP：non-operation）の単純な繰り返しといった攻撃処理にとって、本質的とはいえない部分の構造を検出するようにしてきた。そのため、攻撃データのバリエーションに弱く、未知の攻撃データが現れる毎に、検出に用いるビットパターンのデータベースを更新する必要がある、データベースが更新されるまでのタイムラグが問題になっていた。

【0007】

本発明は斯かる事情に鑑みてなされたものであり、分岐命令に係る命令コードを入力されたデータから検索し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する構成とすることにより、不正な処理を行う命令コード群を検出するためのビットパターンを予め用意する必要がなく、不正な処理を行う未知の命令コード群に対しても検出可能なデータ処理方法、データ処理装置、該データ処理装置を実現するためのコンピュータプログラム、及び該コンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】

第1発明に係るデータ処理方法は、複数の命令コードを含むデータの入力を受け付け、受け付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理方法において、分岐命令に係る命令コードを前記データから検索し、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記

憶し、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断し、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断することを特徴とする。

【0009】

第2発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、分岐命令に係る命令コードを前記データから検索する手段と、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶する手段と、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断する手段と、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶する手段と、記憶した呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断する手段と、前記呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にある場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

【0010】

第3発明に係るデータ処理装置は、第2発明に係るデータ処理装置において、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備え、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力すべくなくしてあることを特徴とする。

【0011】

第4発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、所

定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断する手段と、前記文字列が前記復帰先アドレスに対応付けられている場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

【0012】

第5発明に係るデータ処理装置は、複数の命令コードを含むデータの入力を受け付ける手段を備え、該手段にて受付けたデータに含まれる命令コードに基づいて実行される処理が不正処理であるか否かを判断するデータ処理装置において、所定の処理を実行する命令コード群を呼出するための命令コードを前記データから検索する手段と、前記命令コードが検索された場合、前記命令コード群の復帰先アドレスを取得するための命令コードが前記命令コード群に含まれるか否かを判断する手段と、前記命令コードが前記命令コード群に含まれる場合、前記データが不正処理を実行するデータである旨の情報を出力する手段とを備えることを特徴とする。

【0013】

第6発明に係るコンピュータプログラムは、コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムにおいて、コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有することを特徴とする。

【0014】

第7発明に係るコンピュータでの読取りが可能な記録媒体は、コンピュータに、入力された複数の命令コードを含むデータに基づいて実行される処理が不正処理であるか否かを判断させるステップを有するコンピュータプログラムが記録されているコンピュータでの読取りが可能な記録媒体において、コンピュータに、分岐命令に係る命令コードを前記データから検索させるステップと、コンピュータに、検索された命令コードに対応付けられている分岐元アドレス、及び前記命令コードの分岐先に対応付けられている分岐先アドレスを記憶させるステップと、コンピュータに、前記分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断させるステップと、コンピュータに、前記分岐先アドレスに前記命令コードが対応付けられていると判断した場合、前記命令コードの呼出先アドレスを記憶させるステップと、コンピュータに、記憶させた呼出先アドレスが前記分岐元アドレス及び分岐先アドレスの間にあるか否かを判断させるステップと有するコンピュータプログラムが記録されていることを特徴とする。

【0015】

第1発明、第2発明、第6発明、及び第7発明にあつては、分岐命令に係る命令コードを入力されたデータから検索し、検索された命令コードの分岐元アドレス及び分岐先アドレスを記憶し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出するための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが分岐元アドレス及び分岐先アドレスの間にあるか否かを判断するようにしている。したがって、通常のデータ（実行コード）には見られない普遍的な構造に着目しているため、不正コードを変形させた場合であっても検出できる可能性が高く、未知の攻撃データが現れたときでも、不正コードの本質的処理が変わらない限り、不正コードを見抜くことができる。また、命令コードを逐次的に読込むことによって、不正コードであるか否かの判定が可能であるため処理速度が速く、例えば通信により受信したデータに対してリアルタイムに判定することができる。

【0016】

第3発明にあっては、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備えているため、不正コードの検出精度が向上する。

【0017】

第4発明にあっては、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

【0018】

第5発明にあっては、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、前記命令コードが検索された場合、命令コード群に復帰先アドレスを取得するための命令コードが含まれるか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

【0019】

【発明の実施の形態】

以下、本発明をその実施の形態を示す図面に基づいて具体的に説明する。

実施の形態1.

図1は本発明のデータ処理装置を利用した侵入検出システムを説明する模式的構成図である。図中10は本発明のデータ処理装置を具体化した中継装置であり、例えば、ルータ、スイッチ、ブロードバンドルータ等のデータ通信を中継する装置である。中継装置10は、CPU11、メモリ12、及び通信インターフェース（以下、通信IFという）13、14を備えており、通信IF13に接続された情報処理装置20とインターネット網のようなデータ通信網Nを介して通信IF14に接続された他の情報処理装置30と間で、各種データの送受信を中継する。情報処理装置20、30は、例えば、パーソナルコンピュータ、サーバ装置、携帯電話機、PDA（Personal Digital Assistant）等のデータ通信を行うことができる装置である。

情報処理装置30から送信されたデータを中継装置10が受信した際、中継装

置 10 は受信したデータが不正な処理を実行する命令コード（以下、不正コードという）を含んだデータであるか否かを判断し、不正コードを含んでいる場合には、通信の遮断、警報の出力等の処理を行う。

【0020】

中継装置 10 のメモリ 12 は、ルーティングテーブル 12 a、フィルタリングテーブル 12 b、及び分岐テーブル 12 c を備えている。

ルーティングテーブル 12 a には通信の経路制御情報が記憶されており、該経路制御情報によって、情報処理装置 20 から送信されるデータの伝送経路が決定される。フィルタリングテーブル 12 b には受信を拒否すべき通信相手の識別情報（例えば、IP アドレス又はポート番号等）が記憶されており、前記識別情報に該当する情報処理装置からのデータを受信した場合、そのデータを情報処理装置 20 へ送信しないようにしている。

また、メモリ 12 には本発明のコンピュータプログラムが予め記憶されており、CPU 11 が当該コンピュータプログラムを実行することによって、中継装置 10 は、不正コードを検出する侵入検出システムとして動作する。分岐テーブル 12 c には、前記コンピュータプログラムが起動中に取得した特定の命令コードに係るメモリアドレス（以下、単にアドレスという）が記憶され、不正コードを含んだデータであるか否かを判断する際に利用される。

中継装置 10 の CPU 11 は、これらのテーブルに対して適宜書込み処理、又は読み込み処理を行い、通信制御を行うようにしている。

【0021】

以下、発明者らの知見に基づいて見出された不正コードの特徴的構造について説明する。発明者らは不正コードの普遍的な特徴として、分岐命令（以下、jmp 命令という）により指定された分岐先に呼出命令（以下、call 命令という）が設定されていること、そしてその呼出先が jmp 命令と call 命令との間にあることを見出している。そして、call 命令によって、スタックへ格納されたアドレス、すなわち call 命令の次のアドレスを呼出し先の命令コード群にて取得して、取得したアドレスを用いて起動したいコマンドを実行させるようにしている。

【0022】

図2及び図3は、不正コードの特徴的構造を説明する概念図である。前述したように、処理を分岐させるためのj m p命令の分岐先に対応させてc a l l命令を設定している。すなわち、j m p命令の分岐先アドレス(A 1 0)にc a l l命令に対応させている。

そして、c a l l命令の呼出し先に、外部コマンドを呼び出すための命令コード群(A 2 ~ A 6)を対応付け、そのc a l l命令による呼出し先が、分岐元アドレス(A 1)と分岐先アドレス(A 1 0)との間にくるように設定している。この命令コード群において、c a l l命令によってスタックへ格納されたアドレス、すなわちc a l l命令の次のアドレス(A 1 1)をp o p命令によって取得し、取得したアドレスを利用して、外部コマンドを実行させるようにしている。

したがって、不正コードの作成者が意図した任意の外部コマンドをc a l l命令の次のアドレスに対応させることによって、これらの命令コードが実行されるときに、前記外部コマンドが呼出されて実行される構成となっている。

なお、前記命令コード群とc a l l命令との間(A 7 ~ A 9)にはダミーの初期データ及び作業領域を設けても良いことは勿論である。

【0023】

前述した不正コードは、図3に模式的に示した如く、(1) j m p命令の分岐先にc a l l命令が存在すること、(2) c a l l命令の呼出先がc a l l命令とj m p命令との間に存在することを特徴としている。

中継装置10では、このような特徴的構造を持つ不正コードを通信I F 14にて受信したデータから検出し、警報を出力するか又は通信の遮断を行うようにしている。

【0024】

以下、前述した特徴的構造をもつ不正コードの検出手順について説明する。図4は本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートであり、図5は侵入検出の際に利用される分岐テーブル12cの一例を示す概念図である。まず、中継装置10のC P U 11は通信I F 14にて受信したデータを1バイト読込む(ステップS1)。そして、C P U 11は、読込んだデータが

j m p 命令か否かを判断する（ステップ S 2）。読込んだデータが j m p 命令である場合（S 2：Y E S）、C P U 1 1 は、その j m p 命令で指定される分岐先のアドレスが、現在位置のアドレスよりも大きいかな否かを判断する（ステップ S 3）。

【0025】

分岐先のアドレスが現在位置のアドレスよりも大きいと判断した場合（S 3：Y E S）、現在位置のアドレス（分岐元アドレス）と分岐先のアドレス（分岐先アドレス）とを対応付けて分岐テーブル 1 2 c に記憶させる（ステップ S 4）。図 2 に示した如きデータの例では、アドレス A 1 のデータを読込んだ場合、そのデータは j m p 命令であり、当該 j m p 命令で指定される分岐先のアドレス（A 1 0）がアドレス A 1 よりも大きいため、分岐元アドレスとして A 1、分岐先アドレスとして A 1 0 が分岐テーブル 1 2 c に記憶される（図 5 参照）。

【0026】

ステップ S 3 にて、分岐先アドレスが現在位置のアドレスよりも小さいと判断した場合（S 3：N O）、又はステップ S 4 にて、分岐テーブル 1 2 c に分岐元アドレスと分岐先アドレスとを記憶させた場合、C P U 1 1 は、読込むべきデータが終了したかな否かを判断し（ステップ S 5）、読込むべきデータが未だ残っていると判断した場合（S 5：N O）、処理をステップ S 1 へ戻し、読込むべきデータが終了したと判断した場合（S 5：Y E S）、本ルーチンを終了する。

【0027】

ステップ S 2 において、読込んだデータ j m p 命令でないと判断した場合（S 2：N O）、C P U 1 1 は、現在位置のアドレスが分岐テーブル 1 2 c に記憶された分岐先アドレスに一致するか否かを判断する（ステップ S 6）。現在位置のアドレスが分岐先のアドレスに一致しない場合（S 6：N O）、現在位置のアドレスより小さい分岐先アドレスを分岐テーブル 1 2 c から削除する（ステップ S 7）。そして、ステップ S 5 の処理を行い、再度ステップ S 1 へ処理を戻すか、又は本ルーチンの処理を終了するか否かの判断をする。

【0028】

現在位置のアドレスが分岐テーブル 1 2 c に記憶された分岐先アドレスに一致

すると判断した場合（S6：YES）、CPU11は、現在位置のアドレスに対応付けられた命令コードがcall命令であるか否かを判断する（ステップS8）。現在位置のアドレスに対応付けられた命令コードがcall命令であると判断した場合（S8：YES）、CPU11は、分岐テーブル12cを参照することによって、前記call命令による呼出先が分岐元アドレスと分岐先アドレスとの間にあるか否かを判断する（ステップS9）。

ステップS8にて、call命令でないと判断した場合（S8：NO）、又はステップS9にて、呼出先が分岐元アドレスと分岐先アドレスとの間にないと判断した場合（S9：NO）、処理をステップS5へ移行させる。

【0029】

call命令による呼出先が分岐テーブル12cに記憶された分岐元アドレスと分岐先アドレスとの間にあると判断した場合（S9：YES）、CPU11は、不正コードを検出した旨の情報を生成する（ステップS10）。

【0030】

前述の不正コードを検出した旨の情報は、中継装置10に液晶ディスプレイ等の表示部を設けて表示させるようにしてもよく、また、ブザー、LEDランプ等の警報部を設けて報知するようにしてもよい。更に、前記情報を情報処理装置20へ送信し、情報処理装置20が備える表示部（不図示）にて表示させるようにしてもよい。更に、前記不正コードを検出した旨の情報が生成されたことを受けて通信を遮断するようにしてもよい。

【0031】

なお、前述したようにcall命令によりスタックへ格納されるアドレスには、実行させたい外部コマンドの文字列が存在するため、call命令の次のアドレスにアスキー文字列（コマンド名）が存在するか否かを傍証として利用することにより、不正コードの検出精度を向上させることができる。

また、call命令の次のアドレスにアスキー文字列が存在するか否かについての判断を単独で行うことによっても、不正コードの有無を検出できることが発明者らの検討により知られている。

【0032】

このように、本実施の形態では、データを逐次的に読込んで処理することにより、不正コードが含まれているか否かについて判断できるため、不正コードの有無を検出するアルゴリズムが簡単であり、しかも高速処理が可能である。

【0033】

実施の形態2.

前述の不正コードでは、call命令の次のアドレスに実行させたい外部コマンドを置くこと特徴としており、実施の形態1では、そのような外部コマンドを呼出するための特殊な構造を見出すことによって、不正コードを検出していた。しかしながら、実行させたい外部コマンドは必ずしもcall命令の次に置く必要はなく、不正コードの作者によって予め定められたアドレス分だけ位置をずらして置くことも可能である。このような不正コードをここでは偽装された不正コードと呼び、以下、この偽装された不正コードの特徴的構造、及び検出手順について説明する。なお、中継装置10の構成、及び情報処理装置20、30との接続構成は実施の形態1と同様であるため説明を省略する。

【0034】

図6及び図7は偽装された不正コードの特徴的構造を説明する概念図である。偽装された不正コードでも、call命令によって呼出された命令コード群において、起動したい外部コマンドに対応付けられているアドレスを取得するようにしていることは前述と同様であるが、call命令と外部コマンドとの間に固定長を有するダミーの命令コードを置いて偽装していることが実施の形態1で説明した不正コードと異なる。

すなわち、図6に示した構造を有する偽装された不正コードでは、call命令によりスタックへ格納されたアドレス(A2)を、A16～A20に規定された命令コード群にて取得し、そのアドレスA2から5つ目のアドレス(A7)に対応付けられている外部コマンドを起動させるようにするのである。

【0035】

このような偽装された不正コードは、実施の形態1で説明した処理によっては検出不可能であるが、図7に模式的に示した如く、(1) call命令によって命令コード群を呼出し、(2) その命令コード群において、call命令によっ

てスタックへ格納したアドレスを `pop` 命令により取得するという特徴的構造を依然として有していることが分かる。したがって、`call` 命令によって呼出された命令コード群において、`push` 命令が先行しない `pop` 命令を検索することによって、偽装された不正コードを検出することが可能となる。

【0036】

以下、偽装された不正コードの検出手順について説明する。

図8は本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートである。まず、中継装置10のCPU11は、受信したデータから `call` 命令を検索する(ステップS21)。そして、検索の結果、`call` 命令があるか否かを判断し(ステップS22)、`call` 命令がある場合(S22: YES)、CPU11は、検索された `call` 命令のアドレスをメモリ12に記憶させる(ステップS23)。受信したデータに `call` 命令がない場合(S22: NO)、本侵入検出システムによる処理を終了する。

【0037】

検索された `call` 命令のアドレスを記憶させた後、その `call` 命令により指定される呼出先アドレスへ移動させ(ステップS24)、データを1バイト読込む(ステップS25)。

次いで、CPU11は、読込んだデータがスタックへアドレスを格納するための `push` 命令か否かを判断する(ステップS26)。 `push` 命令であると判断した場合(S26: YES)、現在アドレスを記憶して(ステップS27)、処理をステップS25へ戻す。

【0038】

読込んだデータが `push` 命令でないと判断した場合(S26: NO)、`pop` 命令であるか否かを判断する(ステップS28)。 `pop` 命令でないと判断した場合(S28: NO)、呼出先のルーチンが終了したか否かを判断する(ステップS31)。

呼出先のルーチンが終了していないと判断した場合(S31: NO)、処理をステップS25へ戻し、呼出先のルーチンが終了したと判断した場合(S31: YES)、ステップS23にて記憶させたアドレスを参照し、呼出元の次のアド

レスへ移動させ（ステップS32）、call命令を再度検索し直す。

【0039】

ステップS25で読込んだデータがpop命令であると判断した場合（S28：YES）、CPU11は、ステップS27にて記憶させたアドレスを参照することによって、push命令が先行しないpop命令であるか否かを判断する（ステップS29）。push命令が先行しないpop命令でないと判断した場合（S29：NO）、処理をステップS31へ移行する。

【0040】

ステップS25で読込んだデータが、push命令が先行しないpop命令であると判断した場合（S29：YES）、CPU11は、不正コードを検出した旨の情報を生成する（ステップS30）。

【0041】

前述の不正コードを検出した旨の情報は、実施の形態1と同様に、中継装置10に液晶ディスプレイ等の表示部を設けて表示させるようにしてもよく、また、ブザー、LEDランプ等の警報部を設けて報知するようにしてもよい。更に、前記情報を情報処理装置20へ送信し、情報処理装置20が備える表示部（不図示）にて表示させるようにしてもよい。更に、前記不正コードを検出した旨の情報が生成されたことを受けて通信を遮断するようにしてもよい。

【0042】

実施の形態3.

前述の実施の形態では、ルータ、スイッチ、ブロードバンドルータ等のデータ通信で利用される中継装置に本発明を適用した形態について説明したが、パーソナルコンピュータ、サーバ装置、携帯電話機、PDA等の通信機能を有した情報処理装置に適用することも可能である。

【0043】

図9は本実施の形態に係る侵入検知システムの構成を説明する模式図である。図中50は、パーソナルコンピュータのような情報処理装置であり、該情報処理装置50にはルータのような中継装置40を介してデータ通信網Nへ接続されている。情報処理装置50は、データ通信網N及び中継装置40を通じて各種の通

信機器、及び他の情報処理装置からデータを受信するとともに、それらの通信機器、情報処理装置へデータを送信するようにしている。

【0044】

中継装置40には、CPU41、メモリ42、及び通信IF43、44を備えており、メモリ42には、通信の経路制御情報が記憶されたルーティングテーブル42aと、受信を拒否すべき通信相手の識別情報（例えば、IPアドレス又はポート番号等）が記憶されたフィルタリングテーブル42bとを有している。情報処理装置50から外部へデータを送信する際にルーティングテーブル42aにより伝送経路が設定され、外部からデータを受信する際、フィルタリングテーブル42bを参照することにより受信を拒否すべき通信相手であるか否かが判定される。

【0045】

情報処理装置50は、CPU51を備えており、バス52を介して、ROM53、RAM54、表示部55、入力部56、通信部57、補助記憶装置58、及び内部記憶装置59等の各種ハードウェアに接続されている。CPU51は、ROM53に格納された制御プログラムに従って、それらのハードウェアを制御する。RAM54は、SRAM又はフラッシュメモリ等で構成され、ROM53に格納された制御プログラムの実行時に発生するデータを記憶する。

【0046】

表示部55は、CRT、液晶ディスプレイ等の表示装置であり、入力部56は、キーボード、マウス等の入力装置である。表示部55及び入力部56は、例えば、送信すべきデータの入力及び表示をする際に利用される。通信部57は、モデム等の回線終端装置を備えており、中継装置40を介した各種データの送受信を制御する。

【0047】

補助記憶装置58は、本発明のコンピュータプログラム及びデータを記録したFD、CD-ROM等の記録媒体60からコンピュータプログラム及びデータを読取るFDドライブ、CD-ROMドライブ等からなり、読取られたコンピュータプログラム及びデータは、内部記憶装置59に記憶される。内部記憶装置59

に記憶されているコンピュータプログラム及びデータは、RAM 54 に読込まれ、CPU 51 が実行することで本実施の形態に係る情報処理装置 50 として動作する。

なお、本発明のコンピュータプログラムは、記録媒体 60 により提供されるだけでなく、データ通信網 N を通じて提供される形態であってもよいことは勿論である。

【0048】

前述のコンピュータプログラムは、情報処理装置 50 の起動時に自動的に RAM 54 に読込まれる常駐型のプログラムであることが望ましく、通信部 57 にて外部からデータを受信した際に、自動的に不正コードを検出するようにしておくといよい。なお、不正コードの検出手順については、実施の形態 1 及び実施の形態 2 で説明した通りであるので説明を省略する。

【0049】

本実施の形態では、パーソナルコンピュータのような情報処理装置 50 を利用して不正コードを含んだデータを検出する構成としたが、パーソナルコンピュータの他、携帯電話機、PDA、コンピュータゲーム機、車載通信装置、各種の情報家電に適用できることは勿論である。

また、本発明のコンピュータプログラムを FD、CD-ROM 等の記録媒体に記録させて提供することにより、コンピュータウィルスを検出するアプリケーションソフトウェアのパッケージとして提供することも可能である。

【0050】

【発明の効果】

以上、詳述したように、第 1 発明、第 2 発明、第 6 発明、及び第 7 発明による場合は、分岐命令に係る命令コードを入力されたデータから検索し、検索された命令コードの分岐元アドレス及び分岐先アドレスを記憶し、分岐先アドレスに、所定の処理を実行する命令コード群を呼出すための命令コードが対応付けられているか否かを判断し、分岐先アドレスに前記命令コードが対応付けられていると判断した場合、命令コードの呼出先アドレスを記憶し、記憶した呼出先アドレスが分岐元アドレス及び分岐先アドレスの間にあるか否かを判断するようにしてい

る。したがって、通常の実行コードでは見られない普遍的な構造に着目しているため、不正コードを変形させた場合であっても検出できる可能性が高く、未知の攻撃データが現れたときでも、不正コードの本質的処理が変わらない限り、不正コードを見抜くことができる。また、命令コードを逐次的に読込むことによって、不正コードであるか否かの判定が可能であるため処理速度が速く、例えば通信により受信したデータに対してリアルタイムに判定することができる。

【0051】

第3発明による場合は、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かの判断をする手段を更に備えているため、不正コードの検出精度が向上する。

【0052】

第4発明に場合は、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、命令コード群の復帰先アドレスに所定の文字列が対応付けられているか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる。

【0053】

第5発明による場合は、所定の処理を実行する命令コード群を呼出するための命令コードを入力されたデータから検索し、前記命令コードが検索された場合、命令コード群に復帰先アドレスを取得するための命令コードが含まれるか否かを判断するため、不正コードであるか否かの判定が簡単であり、しかも精度良く判定することができる等、本発明は優れた効果を奏する。

【図面の簡単な説明】

【図1】

本発明のデータ処理装置を利用した侵入検出システムを説明する模式的構成図である。

【図2】

不正コードの特徴的構造を説明する概念図である。

【図3】

不正コードの特徴的構造を説明する概念図である。

【図 4】

本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートである。

【図 5】

侵入検出の際に利用される分岐テーブルの一例を示す概念図である。

【図 6】

偽装された不正コードの特徴的構造を説明する概念図である。

【図 7】

偽装された不正コードの特徴的構造を説明する概念図である。

【図 8】

本実施の形態に係る侵入検出システムの処理手順を説明するフローチャートである。

【図 9】

本実施の形態に係る侵入検知システムの構成を説明する模式図である。

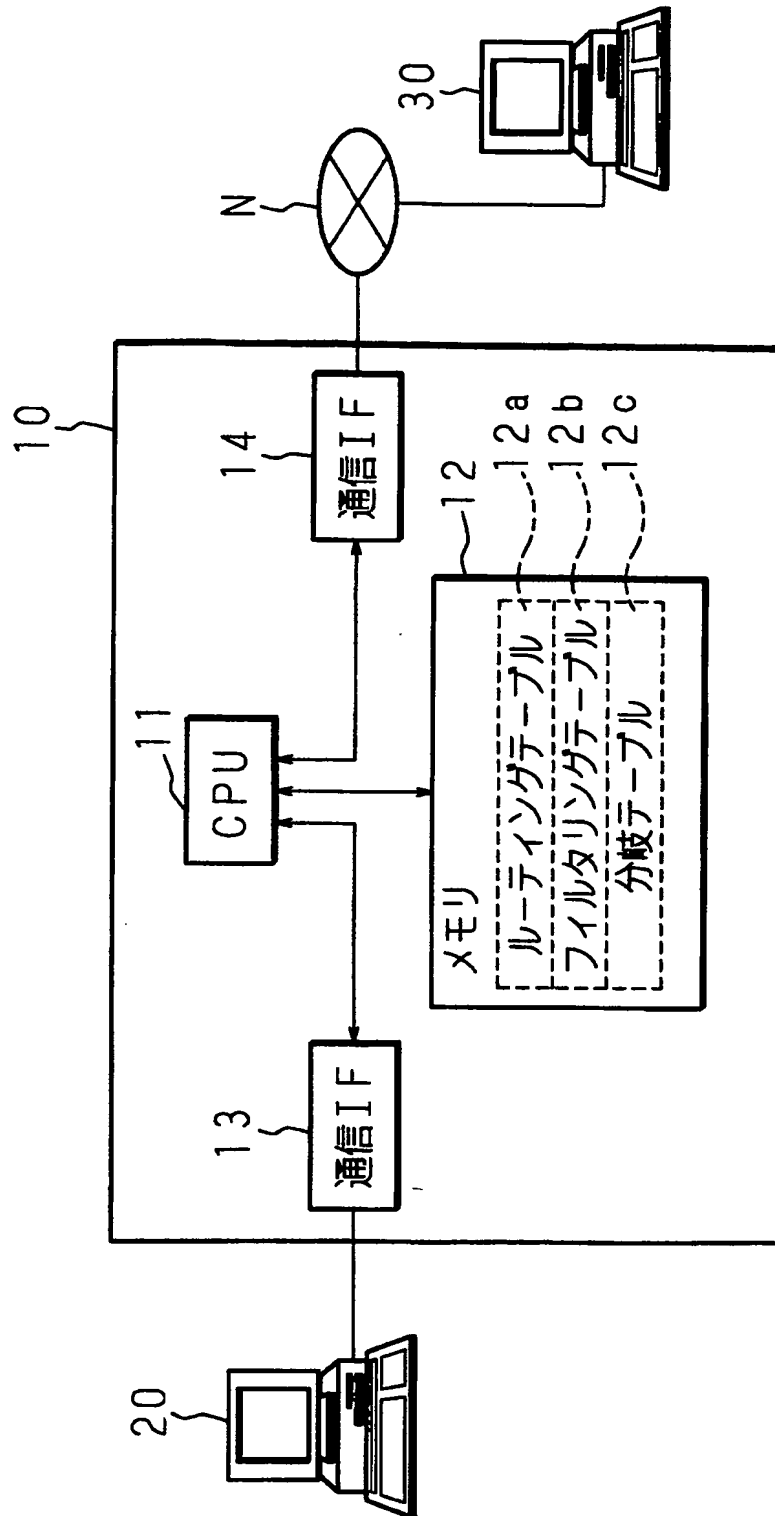
【符号の説明】

- 10 中継装置
- 11 CPU
- 12 メモリ
 - 12a ルーティングテーブル
 - 12b フィルタリングテーブル
 - 12c 分岐テーブル
- 13 通信 I/F
- 14 通信 I/F
- 20 情報処理装置
- 30 情報処理装置
- 50 情報処理装置
- N データ通信網

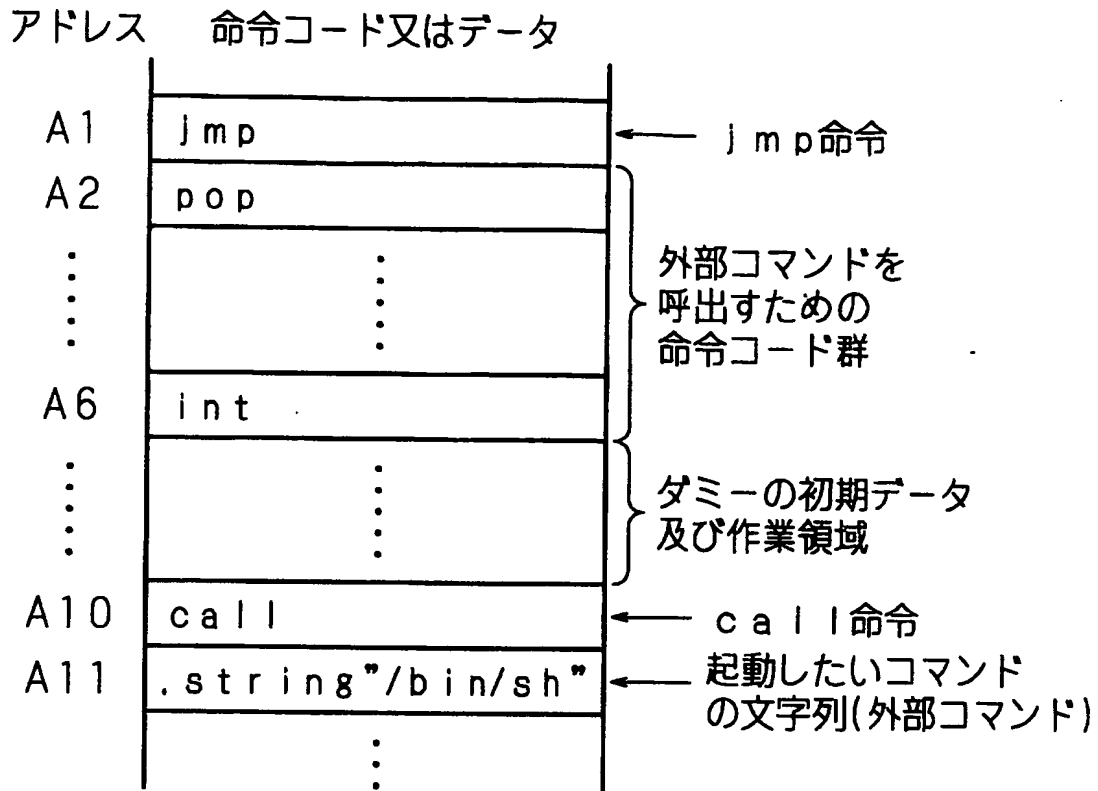
【書類名】

図面

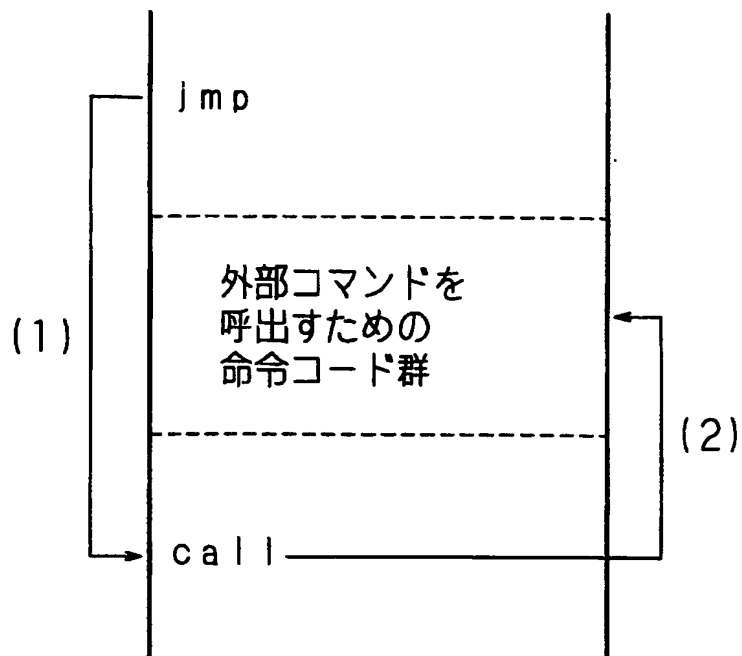
【図 1】



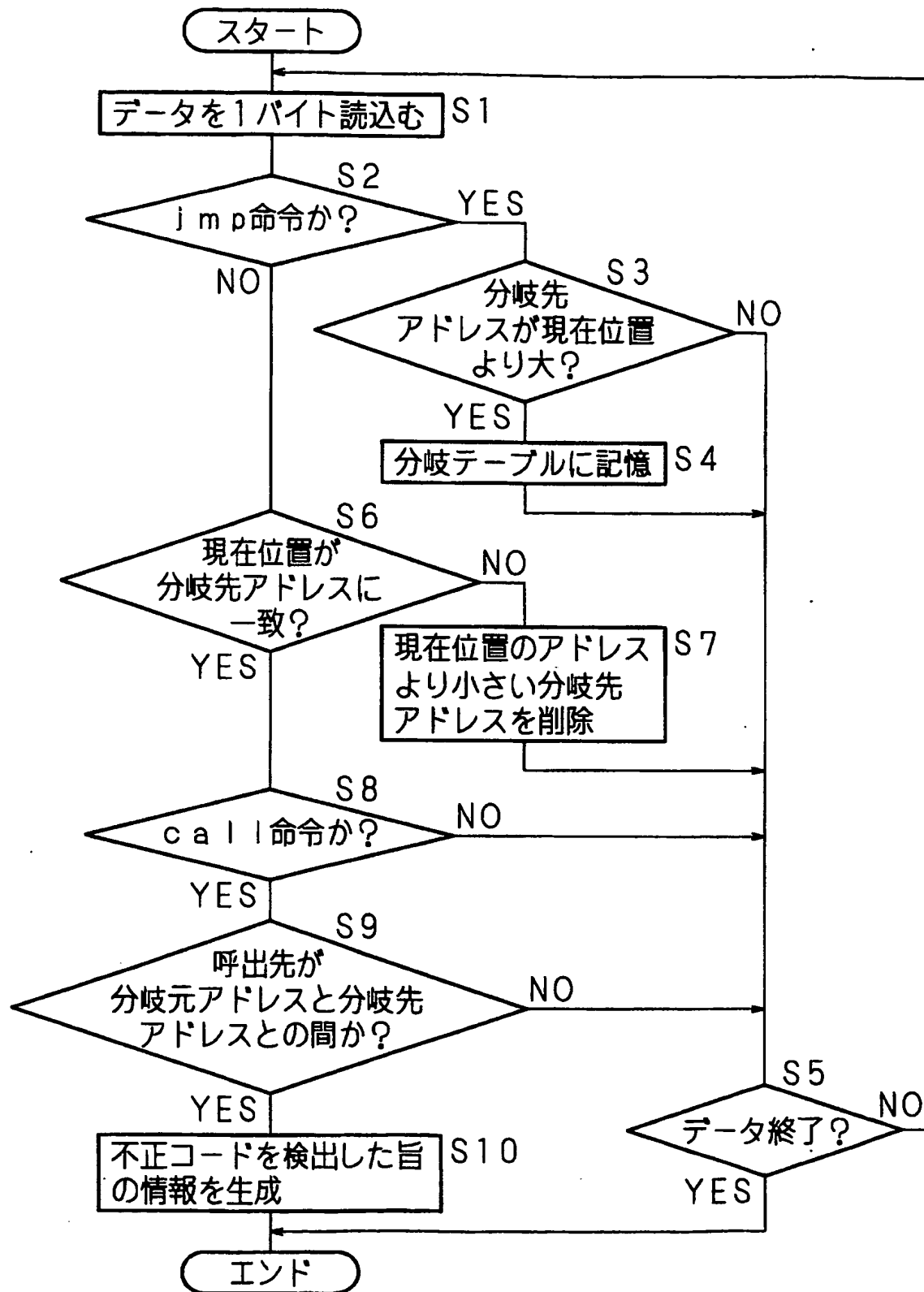
【図2】



【図3】



【図 4】

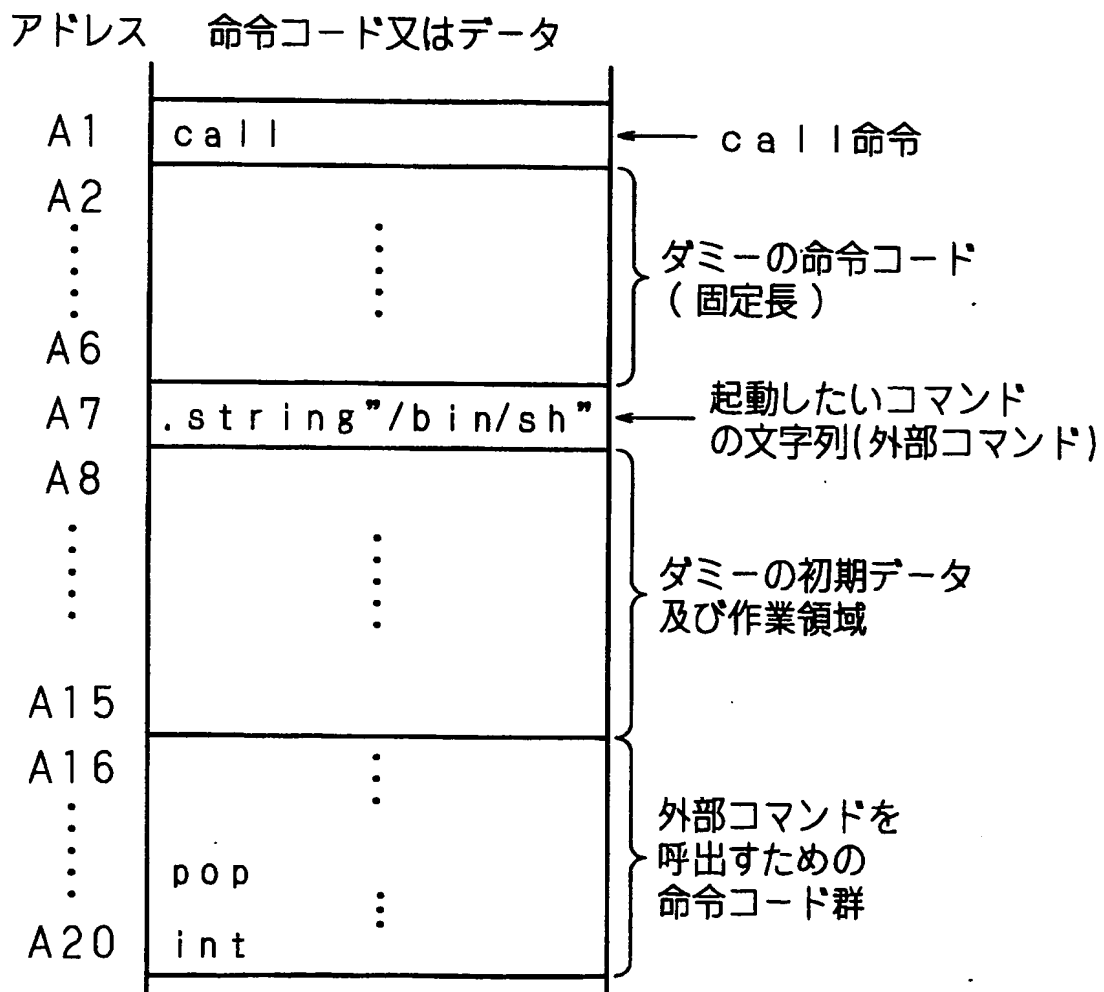


【図5】

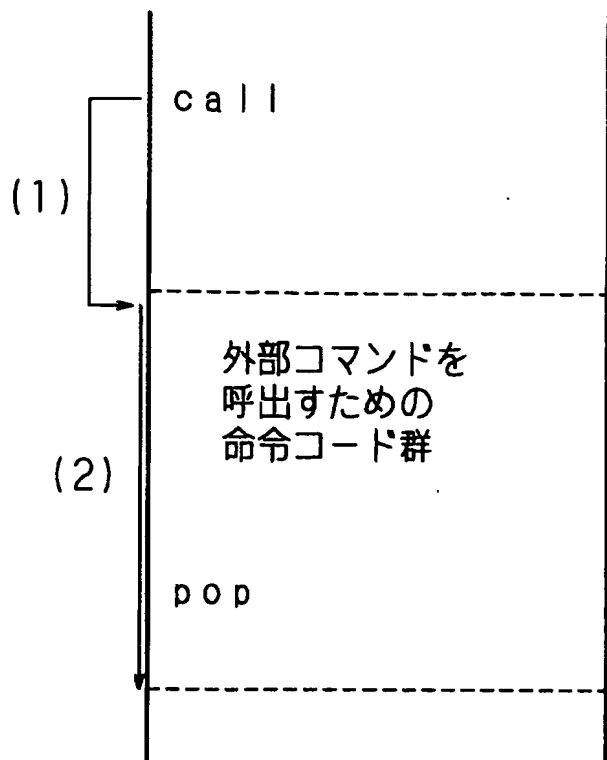
12c

分岐元アドレス	分岐先アドレス
A1	A10
⋮	⋮

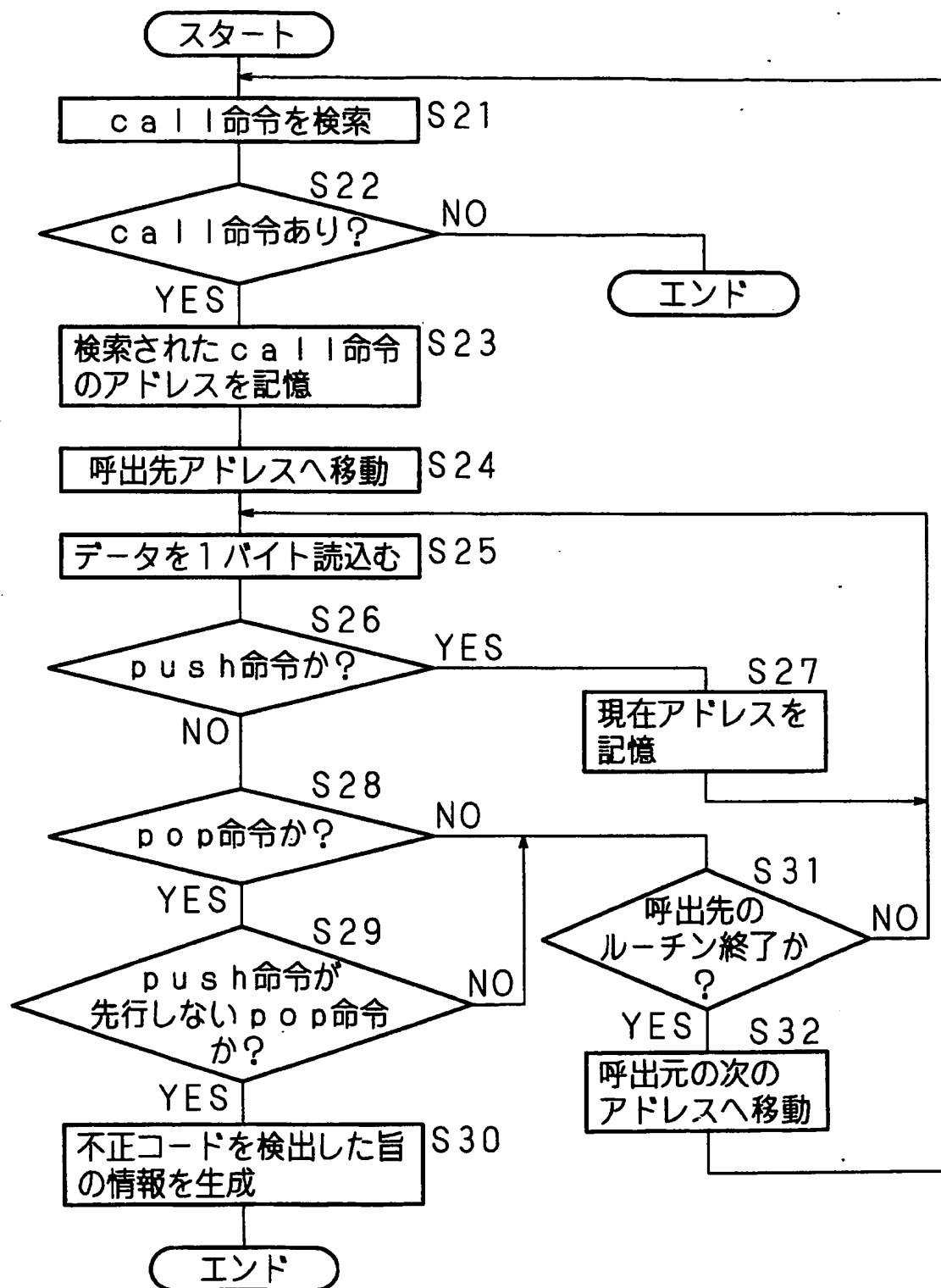
【図6】



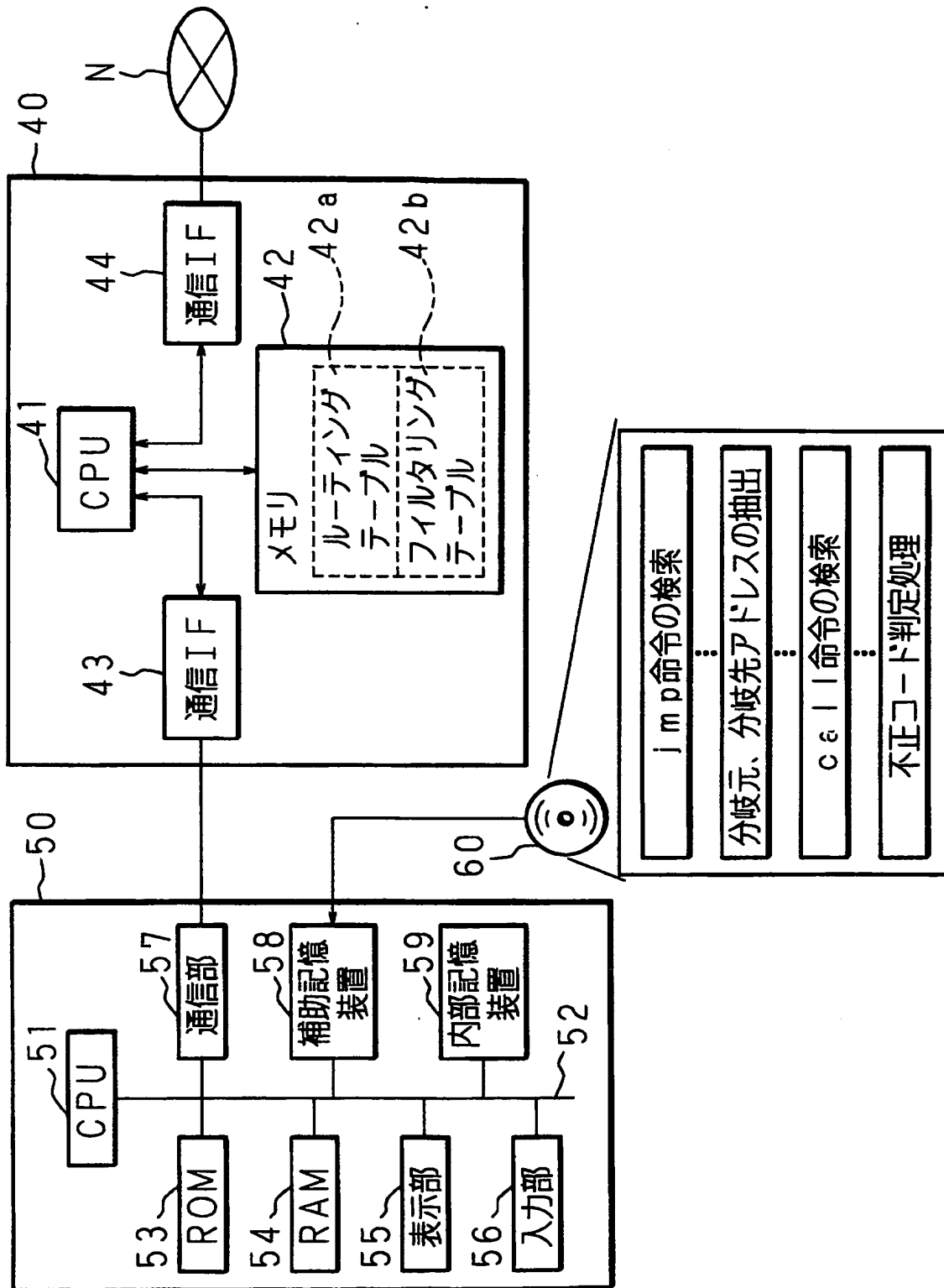
【図 7】



【図8】



【図9】



【書類名】 要約書

【要約】

【課題】 不正コードの本質的構造を見抜いて検出することができるデータ処理方法、データ処理装置、コンピュータプログラム、及び記録媒体の提供。

【解決手段】 分岐命令（j m p 命令）の分岐元アドレスと分岐先アドレスとを記憶し（S 4）、分岐先アドレスに外部コマンドを実行させるための命令コード群を呼出すための呼出命令（c a l l 命令）が対応付けられているか否かを判断し（S 6）、呼出命令が分岐先アドレスに対応付けられている場合、その呼出先が分岐元アドレスと分岐先アドレスとの間にあるか否かを判断し（S 9）、呼出命令による呼出先が分岐元アドレスと分岐先アドレスとの間にある場合、不正コードを検出した旨の情報を生成する（S 10）。

【選択図】 図 4

特願 2002-227888

出 願 人 履 歴 情 報

識別番号

[801000061]

1. 変更年月日

2001年 9月13日

[変更理由]

新規登録

住 所

大阪府大阪市中央区本町橋2番5号 マイドームおおさか内

氏 名

財団法人大阪産業振興機構

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINE(S) OR MARK(S) ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.